



#4  
Dkt. 64498/JPW/PT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Masanori Kusunoki  
Serial No.: 09/805,284  
Filed : March 13, 2001  
For : SYSTEM FOR AUTHENTICATING ACCESS TO A NETWORK,  
STORAGE MEDIUM, PROGRAM AND METHOD FOR  
AUTHENTICATING ACCESS TO A NETWORK

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

TRANSMITTAL OF CERTIFIED COPIES OF EARLIER FILED FOREIGN  
APPLICATIONS AND CLAIM TO PRIORITY PURSUANT TO 35 U.S.C. §119

Applicant submits herewith certified copies of Japanese Patent Application Nos. 2000-069079 and 2001-061999 filed in Japan on March 13, 2000 and March 6, 2001, respectively, and cited in Applicant's Declaration pursuant to 37 C.F.R. §1.63.

Applicant hereby claims the benefit of the March 13, 2000 and March 6, 2001 filing dates pursuant to 35 U.S.C. §119 and 37 C.F.R. §1.55(a).

Respectfully submitted,

John P. White  
Registration No. 28,678  
Paul Teng  
Registration No. 40,837  
Attorneys for Applicant  
Cooper & Dunham LLP  
1185 Avenue of the Americas  
New York, New York 10036  
(212) 278-0400

I hereby certify that this paper is being deposited this date with the U.S. Postal Service with sufficient postage as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

  
Paul Teng  
Reg. No. 40,837

July 12, 2001  
Date

印



# 日本国特許庁

PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日

Date of Application:

2000年 3月13日

出願番号

Application Number:

特願2000-069079

出願人  
Applicant(s):

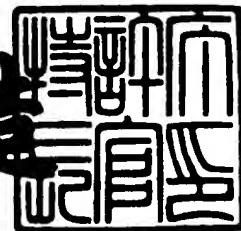
ヤフー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 3月23日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 A000001028

【提出日】 平成12年 3月13日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/00

【発明の名称】 アクセス認証システム及びアクセス認証方法

【請求項の数】 7

【発明者】

    【住所又は居所】 東京都渋谷区恵比寿 1 - 2 4 - 1 6   ピー・アイ・エム  
                                株式会社内

    【氏名】 楠 正憲

【特許出願人】

    【住所又は居所】 兵庫県神戸市中央区港島南町 1 - 5 - 2

    【氏名又は名称】 ピー・アイ・エム株式会社

【代理人】

    【識別番号】 100058479

    【弁理士】

    【氏名又は名称】 鈴江 武彦

    【電話番号】 03-3502-3181

【選任した代理人】

    【識別番号】 100084618

    【弁理士】

    【氏名又は名称】 村松 貞男

【選任した代理人】

    【識別番号】 100068814

    【弁理士】

    【氏名又は名称】 坪井 淳

【選任した代理人】

    【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス認証システム及びアクセス認証方法

【特許請求の範囲】

【請求項 1】

第 1 のターミナルサーバを経由してクライアントに第 2 のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第 1 のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第 1 のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第 1 のチケットデータを作成し、上記第 2 のターミナルサーバに転送する第 1 の認証サーバと、

上記クライアントパラメータの正当性及び上記第 1 のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第 2 のチケットデータを作成し、この第 2 のチケットデータと上記第 1 のチケットデータとを照合し、上記第 2 のターミナルサーバへ上記クライアントの接続可否を指示する第 2 の認証サーバとを備えていることを特徴とするアクセス認証システム。

【請求項 2】

上記所定の規則は、一方向関数による要約であることを特徴とする請求項 1 に記載のアクセス認証システム。

【請求項 3】

上記クライアントパラメータには、上記クライアントの ID、アクセス元 IP アドレス、上記第 1 のチケットデータの有効期限のうち少なくとも 1 つが含まれていることを特徴とする請求項 1 に記載のアクセス認証システム。

【請求項 4】

上記第 1 及び第 2 の認証サーバにおいて、上記第 1 及び第 2 のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする請求項 1 に記載のアクセス認証システム。

【請求項 5】

上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする請求項4に記載のアクセス認証システム。

【請求項6】

第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証方法において、

上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1の認証ステップと、

上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1チケットデータ作成ステップと、

上記第2のターミナルサーバに上記クライアントパラメータ及び上記第1のチケットデータを転送するデータ転送ステップと、

上記第1のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証する検証ステップと、

上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成する第2チケットデータ作成ステップと、

この第2のチケットデータと上記第1のチケットデータとを照合するチケットデータ照合ステップと、

上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証ステップとを備えていることを特徴とするアクセス認証方法。

【請求項7】

第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第1のターミナルサーバに対して上記クライアントから入力されたID及びパスワードに基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ID、上記クライアントのアクセス元IPアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサー

バに転送する第 1 の認証サーバと、

上記第 2 のターミナルサーバに対して上記クライアントから入力されたアクセス元 IP アドレスと上記クライアントパラメータのアクセス元 IP アドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第 1 のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第 2 のチケットデータを作成し、この第 2 のチケットデータと上記第 1 のチケットデータとを照合することで、上記第 2 のターミナルサーバへ上記クライアントの接続可否を指示する第 2 の認証サーバとを備えていることを特徴とするアクセス認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、所定のアプリケーションプロバイダへのアクセス権を予め有するユーザが異なるアプリケーションプロバイダへのアクセス権を得るためのアクセス認証システム及びアクセス認証方法に関する。

【0002】

【従来の技術】

ユーザはインターネットを介して様々な情報サービス等の各種サービスを提供するサービス提供者を利用することができる。サービス提供者とは、インターネットを介して接続されたクライアント端末に対してデータやコンテンツを提供したり、情報処理サービスを提供する業者を指している。サービス提供者はそれぞれ独立しており、ユーザは利用したいサービス提供者と契約し、それぞれ ID とパスワードを持つことでアクセス権を得るようにしている。

【0003】

【発明が解決しようとする課題】

しかし、サービス提供者は増えており、ユーザがそれぞれのサービス提供者と契約するのは ID やパスワードを管理する上で煩雑であった。また、各サービス提供者が提供できるサービスの種類には限界があった。

【0004】

一方、一つのIDとパスワードを複数のサービス提供者間で共通化して用いる方法も考えられるが、ID及びパスワードの両方を各サービス提供者で保持することになるため、課金や秘密保持の点で問題があった。

## 【0005】

そこで本発明は、1つのサーバ（サービス提供者）に対しての個人情報（ID及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することができるようにするためのアクセス認証システム及びアクセス認証方法を提供することを目的としている。

## 【0006】

## 【課題を解決するための手段】

上記課題を解決し目的を達成するために、本発明のアクセス認証システム及びアクセス認証方法は次のように構成されている。

## 【0007】

（1）第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第1のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサーバに転送する第1の認証サーバと、

上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証サーバとを備えていることを特徴とする。

## 【0008】

（2）上記（1）に記載されたアクセス認証システムであって、上記所定の規則は、一方向関数による要約であることを特徴とする。

## 【0009】



(3) 上記(1)に記載されたアクセス認証システムであって、上記クライアントパラメータには、上記クライアントのID、アクセス元IPアドレス、上記第1のチケットデータの有効期限のうち少なくとも1つが含まれていることを特徴とする。

【0010】

(4) 上記(1)に記載されたアクセス認証システムであって、上記第1及び第2の認証サーバにおいて、上記第1及び第2のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする。

【0011】

(5) 上記(4)に記載されたアクセス認証システムであって、上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする。

【0012】

(6) 第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証方法において、上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1の認証ステップと、上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1チケットデータ作成ステップと、上記第2のターミナルサーバに上記クライアントパラメータ及び上記第1のチケットデータを転送するデータ転送ステップと、上記第1のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証する検証ステップと、上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成する第2チケットデータ作成ステップと、この第2のチケットデータと上記第1のチケットデータとを照合するチケットデータ照合ステップと、上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証ステップとを備えていることを特徴とする。

【0013】

(7) 第1のターミナルサーバを経由してクライアントに第2のターミナルサー

バへの接続サービスを行うアクセス認証システムにおいて、上記第1のターミナルサーバに対して上記クライアントから入力されたID及びパスワードに基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ID、上記クライアントのアクセス元IPアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサーバに転送する第1の認証サーバと、上記第2のターミナルサーバに対して上記クライアントから入力されたアクセス元IPアドレスと上記クライアントパラメータのアクセス元IPアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第1のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合することで、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証サーバとを備えていることを特徴とする。

【0014】

#### 【発明の実施の形態】

図1は本発明の一実施の形態に係るアクセス認証システムの構成を示す図、図2の(a)，(b)は同アクセス認証システムに組み込まれた認証サーバ22，32の構成を示すブロック図、図3はアクセス認証の手順を示すフロー図である。なお、本実施の形態はソフトウェア処理により実現する場合も含まれる。

【0015】

図1中10はユーザのクライアント端末、20はユーザと契約関係にあるサービス提供先サービス提供者、30はユーザと直接の契約関係にないサービス提供元サービス提供者、40はインターネット回線、50は電話回線を示している。

【0016】

サービス提供先サービス提供者20は、インターネット回線40に接続されたターミナルサーバ(第1のターミナルサーバ)21と、このターミナルサーバ21に接続され後述するような認証等を行う認証サーバ(第1の認証サーバ)22と、ターミナルサーバ22に接続されるとともに情報サービスを提供するメイン

サーバ 2 3 と、電話回線 5 0 に接続された共通の文字列更新部 2 4 とを備えている。

【 0 0 1 7 】

認証サーバ 2 2 は、第 1 のターミナルサーバ 2 1 に対してクライアント端末 1 0 から入力された ID 及びパスワードに基づいてターミナルサーバ 2 1 のへのクライアント端末 1 0 からの接続の可否を認証する認証部 2 2 a と、クライアント端末 1 0 のアクセス元 IP アドレスを検出する IP アドレス検出部 2 2 b と、後述する第 1 チケット（第 1 のチケットデータ）の有効期限を生成する有効期限生成部 2 2 c と、クライアントパラメータ P、すなわち ID、クライアントのアクセス元 IP アドレス、有効期限生成部 2 2 c で生成された有効期限、共通の文字列更新部 2 4 で更新された最新の共通の文字列を一方向関数で要約する等の所定の規則を用いて第 1 チケットデータ D 1 を作成するチケットデータ生成部 2 2 d と、クライアントパラメータ P 及び第 1 チケットデータを認証サーバ 3 2 にインターネット回線 4 0 及びターミナルサーバ 3 1 を介して転送する転送部 2 2 e とを備えている。

【 0 0 1 8 】

サービス提供元サービス提供者 3 0 は、インターネット回線 4 0 に接続されたターミナルサーバ（第 2 のターミナルサーバ） 3 1 と、このターミナルサーバ 3 1 に接続され後述するような認証等を行う認証サーバ（第 2 の認証サーバ） 3 2 と、ターミナルサーバ 3 1 に接続されるとともに情報サービスを提供するメインサーバ 3 3 と、電話回線 5 0 に接続された共通の文字列更新部 3 4 とを備えている。

【 0 0 1 9 】

認証サーバ 3 2 は、ターミナルサーバ 3 1 に対してクライアント端末 1 0 から入力されたアクセス元 IP アドレスと上述した認証サーバ 2 2 から転送されたクライアントパラメータ P のアクセス元 IP アドレスとを照合するアクセス元 IP アドレス照合部 3 2 a と、有効期限内のアクセスであるか否かを判断する有効期限判断部 3 2 b と、第 1 のチケットデータ D 1 の行使の有無を判断するチケット行使判断部 3 2 c と、転送されたクライアントパラメータ P を上述した規則と同

一の規則で符号化した第2のチケットデータD2を作成するチケットデータ生成部32dと、第2のチケットデータD2と第1のチケットデータD1とを照合することで、第2のターミナルサーバ31へクライアント端末10からの接続可否を指示する認証部32eとを備えている。

#### 【0020】

共通の文字列更新部24及び共通の文字列更新部34は、文字列から構成される同一の共通の文字列を保持しており、定期的に更新されている。

#### 【0021】

このように構成されていると、ユーザがクライアント端末10からメインサーバ33にアクセスする場合には次のように行われる。すなわち、ユーザはクライアント端末10からインターネット回線40を介してターミナルサーバ21に接続を行う。このとき、ユーザはサービス提供先サービス提供者が提供するログイン画面に自己のID及びパスワードを入力する(ST10)。このとき、ターミナルサーバ21では、任意のアクセス制限を行い(ST11)、アクセスが禁止された場合にはログインが拒否される(ST12)。

#### 【0022】

ST2においてアクセスが許可された場合には、ID、パスワード、アクセス元IPアドレスが認証サーバ22に送られ、認証部22aにてID及びパスワードに基づいてユーザ認証を行い(ST13)、認証に失敗した場合にはログインが拒否される(ST14)。なお、この時点でメインサーバ23へのアクセスが許可される。

#### 【0023】

ST4においてユーザ認証が成功した場合には、IPアドレス検出部22bにおいてクライアント端末10のアクセス元IPアドレスが検出され、有効期限生成部22cにおいて第1チケットデータD1の有効期限を生成する。そして、チケットデータ生成部22dにおいて、クライアントパラメータP(ID、アクセス元IPアドレス、有効期限、共通の文字列)を一方向関数で要約して第1チケットデータD1を作成する(ST15)。

#### 【0024】

次に、転送部 2 2 e によりクライアントパラメータ P 及び第 1 チケットデータ D 1 を認証サーバ 3 2 にインターネット回線 4 0 及びターミナルサーバ 3 1 を介して転送する (S T 1 6)。

【 0 0 2 5 】

サービス提供元サービス提供者 3 0 の認証サーバ 3 2 では、アクセス元 I P アドレス照合部 3 2 a によりアクセス元 I P アドレス照合部 3 2 a ターミナルサーバ 3 1 に対してクライアント端末 1 0 から入力されたアクセス元 I P アドレスと上述した認証サーバ 2 2 から転送されたクライアントパラメータ P のアクセス元 I P アドレスとを照合し (S T 2 0)、不一致である場合にはログインは拒否される (S T 2 1)。

【 0 0 2 6 】

次に、有効期限判断部 3 2 b により、有効期限内のアクセスであるか否かを判断し (S T 2 2)、有効期限を経過している場合には無効とされログインは拒否される (S T 2 3)。

【 0 0 2 7 】

次に、チケット行使判断部 3 2 c により、第 1 のチケットデータ D 1 の行使の有無を判断し (S T 2 4)、既に行使されている場合にはログインは拒否される (S T 2 5)。

【 0 0 2 8 】

次に、チケットデータ生成部 3 2 d により、転送されたクライアントパラメータ P を上述した一方向関数で要約した第 2 のチケットデータ D 2 を作成し、第 1 のチケットデータ D 1 とを照合し (S T 2 6)、不一致の場合にはログインは拒否される (S T 2 7)。

【 0 0 2 9 】

次に、I D が既に登録されているものか否かを検索し (S T 2 8)、登録されていれば後述する S T 3 0 に進み、登録されていなければ I D が作成される (S T 2 9)。そして、メインサーバ 3 3 へのログインが可能となる (S T 3 0)。

【 0 0 3 0 】

なお、このようなアクセス認証システムの場合には、サービス提供先サービス

提供者20からサービス提供元サービス提供者30にクライアントパラメータPが転送される際に、何らかの方法でクライアントパラメータPを傍受し、クライアントパラメータPを改竄して不正アクセスしようとしても、第1のチケットデータD1と改竄されたクライアントパラメータPに基づいて作成された第2のチケットデータD2とが不一致となり、ログインが拒否されることになる。

【0031】

なお、改竄されたクライアントパラメータPに基づいて第1のチケットデータD1を作ることにより、新たなサービス提供元サービス提供者30へのログインが可能になる。しかしながら、第1のチケットデータD1の作成には共通の文字列を知る必要がある。しかも、この共通の文字列は、認証サーバ22, 32に侵入して入手したり、総当たり法によって推測したり、一方向関数の逆演算して導き出すことが考えられるが、共通の文字列の更新を十分に短く設定することで、事実上共通の文字列を入手することが困難になる。

【0032】

また、クライアントパラメータP及び第1のチケットデータD1を流用しようとしても、有効期限を十分に短く設定しておけば、有効期限後のアクセスとなる可能性が高く、ログインが拒否されることになる。

【0033】

さらに、有効期限内の使用であっても、正規のユーザによるサービス提供元サービス提供者30へのアクセスは、サービス提供先サービス提供者20へのアクセスとほぼ同時である。このため、クライアントパラメータP及び第1のチケットデータD1を第三者が傍受し不正使用しようとしても、既に正規のユーザによって第1のチケットデータD1の行使が済んでおり、第三者の第1のチケットデータD1ではログインができない。

【0034】

一方、正規なユーザが共通の文字列を含んだ状態で生成された第1のチケットデータD1をサービス提供元サービス提供者30に到達した時点で、共通の文字列が更新されていて第2のチケットデータD2と第1のチケットデータD1が異なってしまうログインが拒絶されてしまう問題は、次のようにして解決する。

## 【0035】

例えば、定期的に A, B, C, D という順番で共通の文字列を変える場合、A B, B C, C D, … というように 2 つの共通の文字列を組み合わせることで、2 種類の第 1 のチケットデータ D 1 を作成し、この 2 つの第 1 のチケットデータ D 1 のいずれかが第 2 のチケットデータ D 2 と一致すればログイン可能とするように設定することにより対処する。

## 【0036】

上述したように、本発明の一実施の形態に係るアクセス認証システムによれば、1 つのサービス提供先サービス提供者に対しての ID 及びパスワードのみで、各種サービスを提供する他のサービス提供元サービス提供者にパスワードを開示することなく利用することが可能となる。また、サービス提供先サービス提供者からサービス提供元サービス提供者に転送されるデータが第三者により傍受された場合であっても、何重にも安全対策が講じられているため、サービス提供元サービス提供者に不正にアクセスがされることがない。

## 【0037】

なお、本発明は前記実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で種々変形実施可能であるのは勿論である。

## 【0038】

## 【発明の効果】

本発明によれば、1 つのサーバ（サービス提供者）に対しての個人情報（ID 及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することが可能となる。

## 【図面の簡単な説明】

## 【図 1】

本発明の一実施の形態に係るアクセス認証システムの構成を示す図。

## 【図 2】

同アクセス認証システムに組み込まれた認証サーバの構成を示すブロック図。

## 【図 3】

同アクセス認証システムの動作を示すフロー図。

【符号の説明】

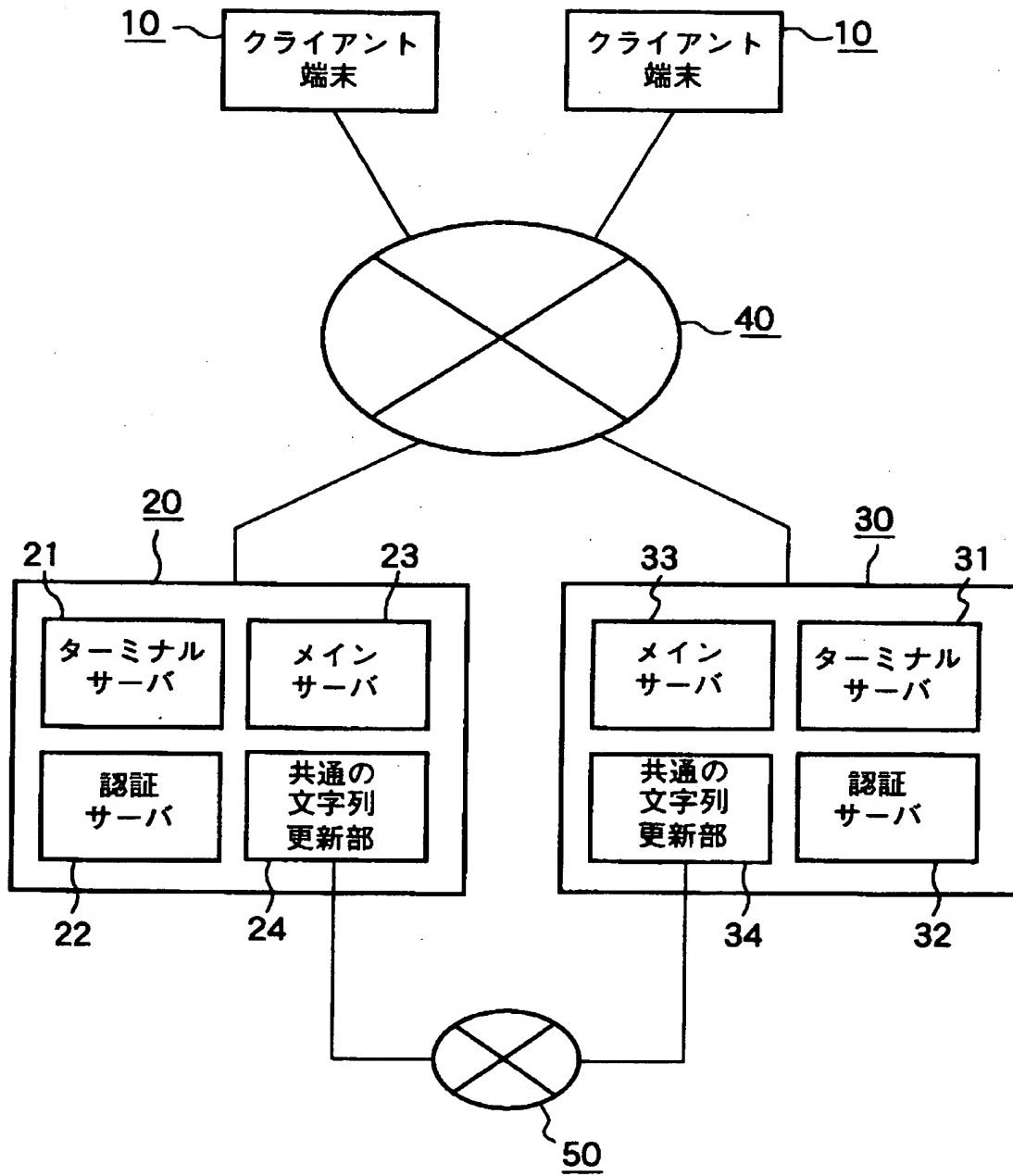
- 1 0 …クライアント端末
- 2 0 …サービス提供先サービス提供者
- 3 0 …サービス提供元サービス提供者
- 4 0 …インターネット回線
- 5 0 …電話回線



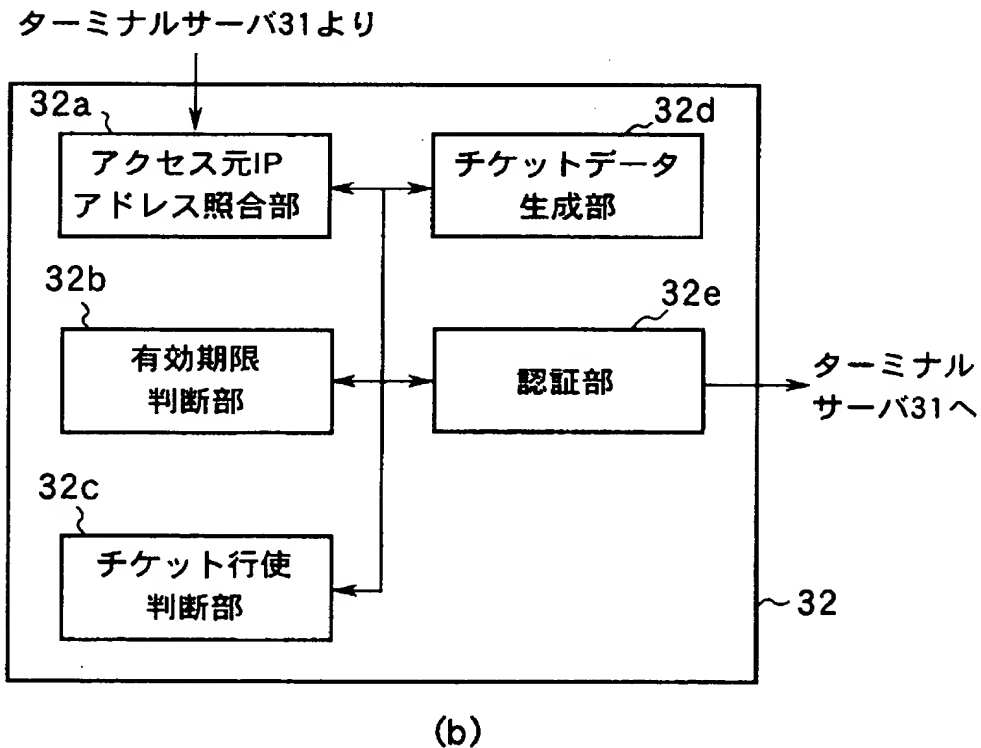
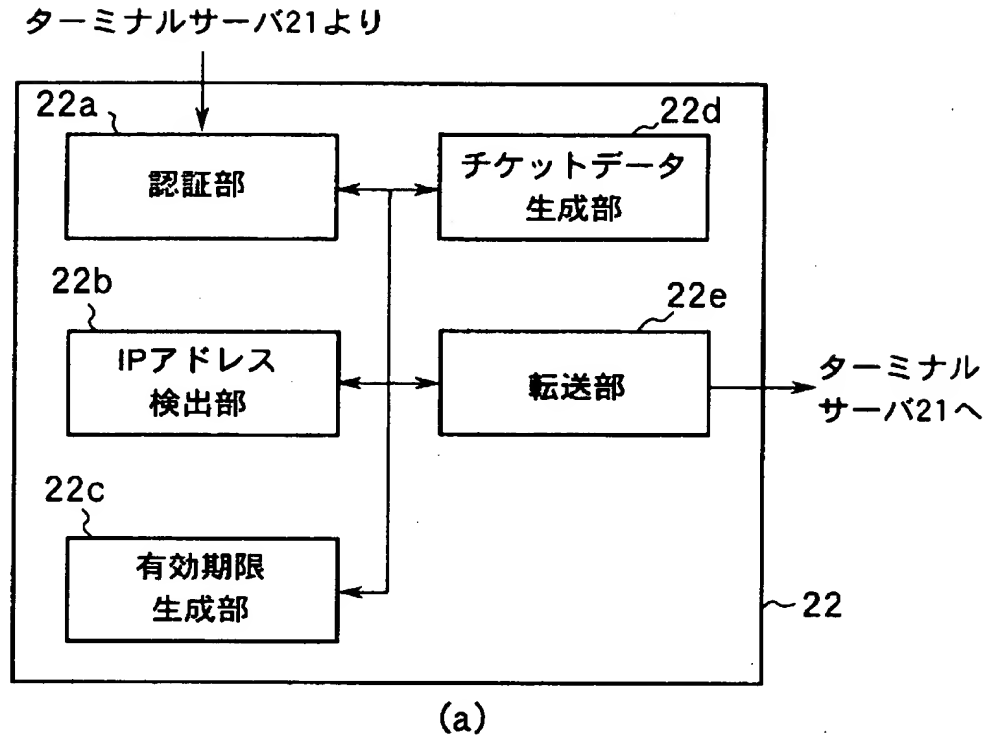
【書類名】

図面

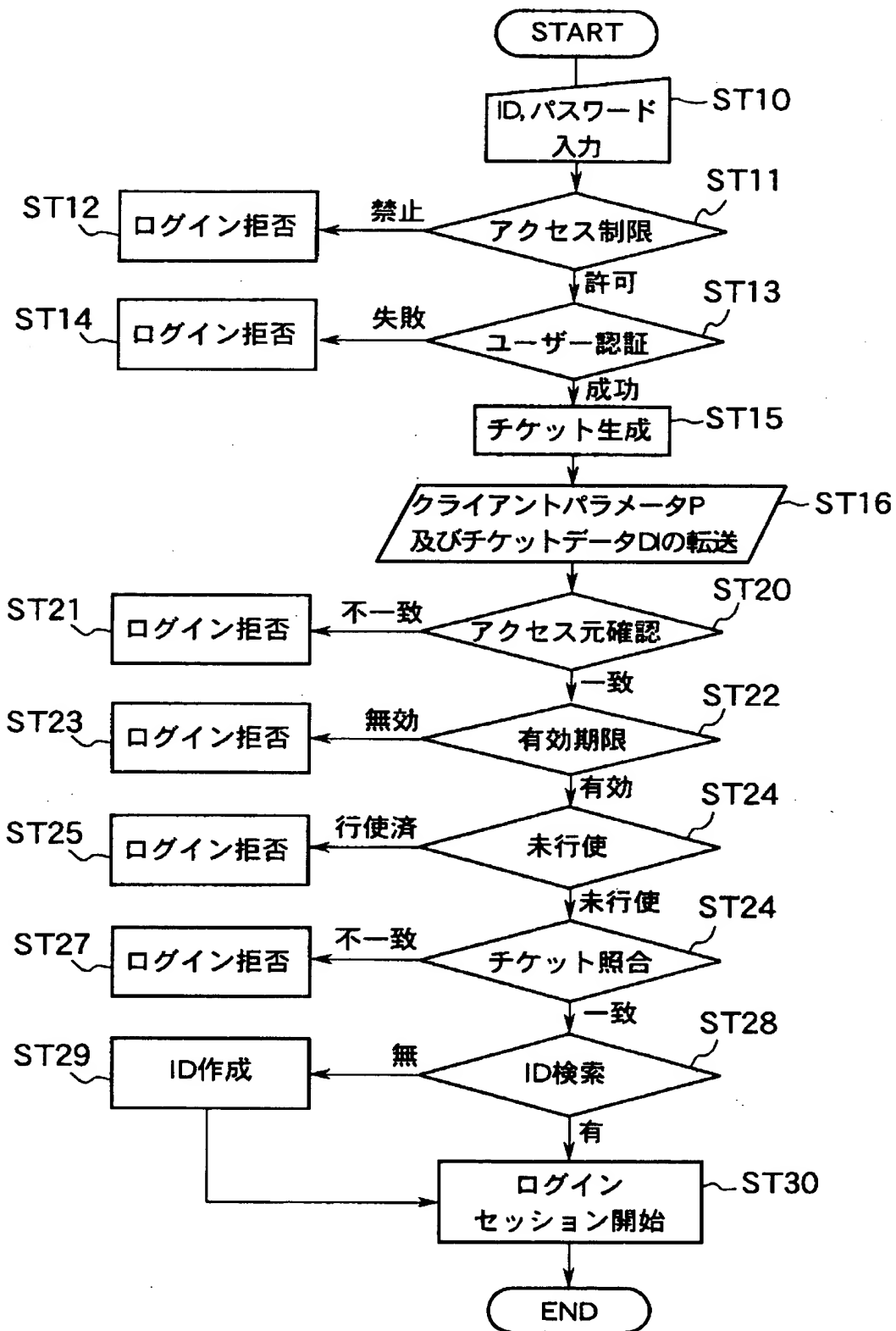
【図1】



【図 2】



【図3】



【書類名】 要約書

【要約】

【課題】 1つのサーバに対しての個人情報に基づいて、各種サービスを提供する他のサーバを利用可能とするアクセス認証システムを提供すること。

【解決手段】 クライアント端末10から入力された個別情報に基づいて第1のターミナルサーバへの接続の可否を認証するとともに、クライアントパラメータPを符号化した第1のチケットデータを作成し、第2のターミナルサーバに転送する第1の認証サーバ22と、クライアントパラメータPの正当性及び第1のチケットデータD1の行使の有無を検証するとともに、クライアントパラメータPを符号化した第2のチケットデータD2を作成し、第2のチケットデータD2と第1のチケットデータD1とを照合し、第2のターミナルサーバ31へクライアント端末10の接続可否を指示する第2の認証サーバ32とを備えている。

【選択図】 図1

【書類名】 出願人名義変更届（一般承継）

【整理番号】 AK00001028

【提出日】 平成12年11月29日

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2000- 69079

【承継人】

【識別番号】 500257300

【氏名又は名称】 ヤフー株式会社

【承継人代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【提出物件の目録】

【物件名】 権利の承継を証明する書面 1

【提出物件の特記事項】 手続補足書に添付して提出する。

【包括委任状番号】 0017007

【ブルーフの要否】 要

認定・付加情報

特許出願の番号	特願2000-069079
受付番号	50001536469
書類名	出願人名義変更届（一般承継）
担当官	濱谷 よし子 1614
作成日	平成13年 3月 8日

<認定情報・付加情報>

【承継人】

【識別番号】	500257300
【住所又は居所】	東京都港区北青山3-6-7
【氏名又は名称】	ヤフー株式会社

【承継人代理人】

申請人

【識別番号】	100058479
【住所又は居所】	東京都千代田区霞が関3丁目7番2号 鈴榮内外 國特許法律事務所内
【氏名又は名称】	鈴江 武彦

出 願 人 履 歴 情 報

識別番号 [500112250]

1. 変更年月日 2000年 3月13日  
[変更理由] 新規登録  
住 所 兵庫県神戸市中央区港島南町1-5-2  
氏 名 ピー・アイ・エム株式会社
2. 変更年月日 2000年11月27日  
[変更理由] 住所変更  
住 所 東京都渋谷区恵比寿一丁目24番16号  
氏 名 ピー・アイ・エム株式会社

出 願 人 履 歴 情 報

識別番号 [500257300]

1. 変更年月日 2000年 6月 2日  
[変更理由] 新規登録  
住 所 東京都港区北青山3-6-7  
氏 名 ヤフー株式会社